

8

October 4, 1935

MEMORANDUM FOR: Research and Development Division.
(THRU: War Plans & Training Division)

1. Attached hereto are draft specifications and six drawings covering a new type of controlling means for cryptographic machines using rotatable commutators. The basic principle is, in my opinion, novel and very valuable. It is exemplified in several embodiments shown in the drawings.

2. This is the joint invention of the undersigned and one of my assistants, Mr. Frank B. Rowlett, Junior Cryptanalyst.

3. It is recommended that patent be applied for at once, to safeguard the government's interest, even though it may not be desirable to allow the patent to go to issue for some time.

William F. Friedman.

Encls.

Draft specifications,
6 drawings.

✓

The object of this invention is to provide new and useful improvements in cipher machines or cryptographic mechanisms utilizing rotatable commutators for enciphering a plain-language message by what is commonly known as a process of substitution, the latter being accomplished in a systematic manner so that the process of substitution may be automatically reversed in deciphering such an enciphered message, thus recovering the original plain-language message.

In the cryptographic mechanisms referred to there is usually provided a keyboard of the typewriter type, which controls a set of switches corresponding to message characters, and a set of signaling devices which may consist of a bank of glow lamps or magnets to indicate the message characters resulting from operation of the keyboard. The set of switches of the keyboard and the set of signaling or indicating devices are connected to each other electrically by circuits and apparatus by means of which the aforesaid substitution is accomplished.

The cryptographic principle of such cryptographic mechanisms, which will hereinafter be termed simply cryptographs, is based on the establishment of a plurality of electrical circuits or paths between the keyboard switches and the indicating devices through commutators of a special type now well known in the art. These commutators are constructed in the form of flat disks bearing an annular set of contacts on each face, individual contacts of one face being connected by insulated conductors passing through the disk to individual contacts of the other face in an arbitrary manner. In the literature of cryptography such commutators are called "cipher wheels", "coding cylinders", and the like; but, for purposes of greater clarity in description they will hereinafter be referred to as "substitution commutators." In a single cryptograph there may be several such commutators juxtaposed on a common shaft. Thus, when more than one substitution commutator is used, the cipher letter obtained upon depressing a key of the keyboard is the result of the passage of an electrical current along a complex path set up through all the juxtaposed substitution commutators, this path being composed of as many sub-paths joined sequentially as there are commutators.

Enclosure 1 (with 6 drawings)

Gryptographs of the foregoing description may be divided into two categories. Into one category may be placed all cryptographs having one or more substitution commutators, rotatably mounted on a shaft between two fixed end plates, each end plate bearing an annular ring of contacts, the latter being so disposed as to coincide exactly with the contacts on the faces of the substitution commutators. In cryptographs falling into this category the keying switches of the manually operated keyboard are connected to the contacts of one of the end plates, while members of the bank of indicating devices are connected to the contacts of the other end plate. Also a reversing switch is provided, which enables the operator to interchange the connections between the two end plates, the bank of indicating devices and the keyboard switches so as to provide for enciphering and deciphering equivalency. Into the other category may be placed all cryptographs having a single end plate of the type described. The latter contacts are, however, connected to the movable members of a set of single pole, double throw switches, the number of switches being the same as the number of contacts provided on the end plate, and so constructed that the switches are controlled by the keys of the manually operated keyboard. Adjacent to the above-described end plate are mounted one or more substitution commutators, the final commutator, that is, the one most remote from the end plate, being what is hereinafter described and referred to as a "reversing commutator". The purpose of the reversing commutator is to return a current entering the commutators at one contact on the end plate to some other contact on the same end plate; the current, ~~going~~ ^{thus comes} into the reversing plate via one complicated path through the commutators and ~~returns~~ ^{returns} to the end plate along another path through the commutators. Thus, in this category of cryptographs enciphering-deciphering equivalency is effected without the use of a reversing switch which is necessary in cryptographs of the first category.

In both categories of cryptographs it is usual to provide means for angularly displacing or rotating the commutators, the reason for which will be briefly discussed. If, in cryptographs utilizing substitution commutators of the type described, no provision is made for their angular displacement during the course of enciphering a plain-text message, the resulting cipher text will be mono-alphabetic in character; that is, only one substitution alphabet will have been

used in the entire encipherment. It is a well-known fact that such monoalphabetic cryptograms offer little resistance to cryptanalysis, and, in order to increase the cryptographic security of such cryptograms, factors other than mere change of alignment of the substitution commutators from message to message must be incorporated therein. Heretofore several types of cipher machines have been invented in which one or more of the substitution commutators are rotated step by step with the encipherment or decipherment of each letter, but in a regular and/or meter-like manner. Such cipher machines provide a considerable increase in cryptographic security (that is, resistance to cryptanalysis) over those cipher machines in which no angular displacement of the substitution commutators takes place, but still not sufficient to insure practical indecryptability for cryptograms produced by their use. This is because the latitude of variability offered by the substitution commutator displacement mechanism is limited and all forms thereof may be readily reconstructed from a model of the cipher machine.

It is the object of this invention to provide a means of effecting the angular displacement or rotation of the substitution commutators in an irregular, completely aperiodic manner, thereby greatly increasing the resistance to cryptanalysis of cryptograms enciphered by cryptographs of the type described.

A basic feature of the invention is the provision of methods and means for controlling the angular displacements of the substitution commutators by electrical circuits which also pass through rotatable commutators. The latter thus constitute, in effect, commutators for the control of the substitution commutators; for sake of brevity and clarity in description, commutators performing this function of controlling substitution commutators will hereinafter be designated simply as "control commutators". Several specific embodiments of the basic invention will be described. At this point it will merely be mentioned that the control commutators may form an independent unit physically separate from the substitution commutators but electrically associated with the latter; it is possible, however, to make one and the same set of commutators serve both as control commutators and

substitution commutators, there being provided associated means designed to keep the control functions electrically separate from the substitution functions.

The several different embodiments of the invention and the modes of operation of the various forms are explained in this specification in detail sufficient for comprehension by those skilled in the art. The explanation is made in connection with the accompanying drawings, Figs. 1 - 6.

Fig. 1 is a schematic diagram of the simplest embodiment in which there is shown a first set of commutators for performing substitution functions and a second set of somewhat differently constructed commutators for performing control functions, together with the associated circuits and contacts for proper operation of the cryptograph. Fig. 2 is a schematic diagram of a set of commutators also designed for performing control functions but in this case these commutators are similar in construction to the substitution commutators. Fig. 3 is a schematic diagram of another embodiment in which a single set of double-ring commutators of novel construction performs both functions of substitution and control. Fig. 4 shows a front and side elevation of one of these double-ring commutators. Fig. 5 is a schematic diagram of another embodiment in which a ~~single~~ set of double-ring commutators is arranged with associated switching mechanism so as to perform both functions of substitution and control, without the use of a reversing commutator. Fig. 6 is a schematic diagram of another embodiment in which single-ring commutators are used for this purpose, one commutator being a reversing commutator.

Referring now specifically to Fig. 1, elements designated by the numbers 1 to 4, inclusive, are substitution commutators of the normal type hereinbefore described, in which there is a single ring of 26 contacts on each face, the contacts on one face being connected irregularly to the contacts on the other face. Commutator 5 is also a substitution commutator, but differs from the others in that only one face of the commutator bears a ring of contacts, the latter contacts being interconnected irregularly in pairs. A current entering one contact of the single ring of contacts is merely carried along on insulated conductor to some other contact, from which it emerges from the commutator. In other words the current enters the commutator at one contact and leaves it at another, on the same face of the commutator. This is a commutator of the type referred to above as a reversing commutator. Commutators 6, 7 and 8 are control commutators of which 7 and 8 are similar in principle to substitution commutators 1 to 4, except that they have only six contacts instead of 26 in a ring

on each face; commutator 6 is a reversing commutator and is similar in principle to reversing commutator 5, except that it has only six contacts instead of 26.

The substitution commutators are mounted upon a common shaft 20 upon which they may be independently angularly displaced stepwise $1/26$ of a revolution, between fixed end plates ~~301 and 302~~ ^{bearing plate 302, the latter} and ~~303 and 304~~ ^{and 303} serving merely as a retaining plate and having no contacts or conductors within it. The commutators are separated by fixed plates 305, 306, 307, and 308 which bear rings of 26 contacts suitably disposed for bridging between successive commutators, in order to provide for electrical continuity from one commutator to its next adjacent one. The contacts in these separator plates are ball-bearing spring contacts exerting sufficient outward pressure to insure good contact. The control commutators are mounted upon the same common shaft 20 upon which they may likewise be angularly displaced stepwise $1/6$ of a revolution, between fixed end plate ~~301~~ ^{bearing plate 303, the latter} and ~~302~~ ^{and 303} serving merely as a retaining plate. 309 and 310 are separators similar in construction and function to separators 305 to 308, except that they have rings of but 6 contacts. The motion of the three control commutators, is meter-like, commutator 8 being moved $1/6$ of a revolution for each character ciphered, commutator 7 being moved $1/6$ of a revolution per complete revolution of commutator 8, and commutator 6 being moved $1/6$ of a revolution per complete revolution of commutator 7. This set of three commutators has a complete period (return to an initial position) of 216; that is, after 216 characters have been enciphered or deciphered the commutators return to their initial relative rotatory positions. The means for moving these commutators will be described presently. 9, 10, 11, 12, and 13 are magnets, here termed substitution-commutator selector magnets, which when energized, determine which of the substitution commutators 1, 2, 3, 4 and 5 are angularly displaced, either by acting directly on the commutators or by releasing an actuating mechanism which acts directly on the commutators. 14 and 15 are two of a set of twenty-six indicating devices such as glow lamps or magnets for operating a printing mechanism, such indicating devices being well known in the art. Each indicating device corresponds to a letter of the English alphabet. 18 and 19 are two of a set of twenty-six single-pole, double-throw

switch levers operated by the keys of a typewriter keyboard. The keyboard is also provided with a universal bar 44, which controls switch lever 17, the functions of which will be described later, and it also controls switch lever 117 and contact 45, which control magnet 31, the latter serving to displace commutator 8 one step per depression of any key of the keyboard. When commutator 8 makes a complete revolution, it closes contact 32 which controls magnet 33, the latter serving to displace commutator 7 one step per 6 depressions of keys on the keyboard. When commutator 7 makes a complete revolution it closes contact 34 which controls magnet 35, the latter serving to displace commutator 6 one step per 36 depressions of the keys of the keyboard. Contacts 32 and 34 are operated by rollers on spring levers. These rollers normally ride upon the peripheries of commutators 7 and 8, but at a certain point on each commutator there is a transverse slot which allows the roller to drop sufficiently to close the contact concerned. Of course, these three commutators could be displaced mechanically, by means of ratchets and pawls and direct control from the universal bar of the keyboard. To the right in Fig. 1 is shown a side elevation of fixed end plate 304 which adjoins control commutator 8 on the exit face of the commutator. The whole lines show the conductors leading away from the 6 contacts on the right side of the end plate 304, the dotted lines show the conductors leading from the left side of end plate 304 into commutator 8.

Having now particular reference to Figure 1 with a view to giving a complete description of the action of this form of the invention, the sequence of events which transpire during the encipherment of the plain-text letters will be related in detail. In order to encipher a message, it is necessary first to mount the commutators upon the shaft according to some prearranged order, it being obvious that commutators 1, 2, 3, and 4 may be interchanged in position amongst themselves, and commutators 7 and 8 may be interchanged; commutators 5 and 6 must remain in the positions shown, since they are reversing commutators and cannot be replaced by the other commutators or by each other. Next it is necessary to align the several commutators, as regards their relative rotatory

positions upon the shaft, according to a prearranged key. After all this has been accomplished, ~~main power~~ switch 36 is closed, setting up a circuit as follows: From battery 16 to ~~switch 36~~ ^{closed} conductor 51, contact lever 17, closed contact 21, conductor 26, contact 27 on the fixed end plate 304, into, through, and out of the control commutator unit via the route through 8, 310, 7, 309, 6, 309, 7, 310, ~~to~~ 8 as indicated to contact 23, thence along conductor 38 to selector magnet 10, conductor 43 and back to battery 16. When magnet 10 is momentarily energized it causes substitution commutator 4 to be displaced angularly through 1/26th of a revolution. The machine is now ready for enciphering. If the letter A is to be enciphered, the key corresponding thereto is depressed. At the beginning of its downward travel the universal bar 44 causes contact lever 17 to move away from contact 21. The key bar A causes contact lever 18 to break contact at 46 and to make contact at 22, setting up a circuit as follows: From battery 16 ~~to~~ ^{closed} along conductor 23 to contact 22, contact lever 18 and conductor 24 to a contact 29 in end plate 301, thence into substitution commutator 1, through the commutators and separators 1, 305, 2, 306, 3, 307, 4, 308, into and out of reversing commutator 5, back through separators and commutators 308, 4, 307, 3, 306, 2, 305, 1, out at contact 30, return along conductor 25 to contact lever 19, contact 47, thence to indicating device 14, which in this drawing corresponds to the letter Q, conductor 43, and back to battery 16. At the end of the downward travel of the universal bar 44, the latter moves switch lever 117 and closes contact 45, momentarily closing the circuit for energizing magnet 31. This causes control commutator 8 to be angularly displaced through 1/6 of a revolution. When key A is released, the universal bar 44 is returned to its normal position by a retractile spring and contact lever 17 returns to contact 21, reestablishing the circuit from battery 16, switch 36, lever 17, contact 21, conductor 26 to contact 27 of fixed end plate 304. ~~Due to the angular displacement of control commutator 8, the current will now~~ ^{Due to the angular displacement of control commutator 8, the current will now} traverse a new path through the control unit and back to some other contact of end plate 304 from whence it passes through one of the selector magnets 9 - 13, to battery 16, causing one of the substitution commutators to be displaced, and thus providing a new substitution alphabet for the encipherment of the next plain-text letter.

The deciphering operation of this machine is the same as the enciphering operation, the enciphering-deciphering relationship being by nature reciprocal. In setting the machine for deciphering, the same procedure is followed as for enciphering; that is, the commutators are arranged and aligned at the bench mark according to the prearranged key and switch 36 is closed, whereupon substitution commutator 4 is angularly displaced as hereinbefore described. The key corresponding to the cipher letter Q is depressed, which causes contact lever 19 to break contact at 47 and to make contact at 42 causing current to flow from battery 16 through conductor 23, ~~closed contact 42,~~ contact lever 19 and conductor 25 to contact 30 on end plate 301 of the substitution commutator unit. The current passes into and through the latter along one path and returns along another path as described before; it emerges at contact 29 on end plate 301 and flows along conductor 24 to contact lever 18, closed contact 46, to indicating device 15, which corresponds to the letter A. The universal bar 44, operated by the depression of the key corresponding to the letter Q, closes contact 45 at the end of its downward travel and causes control commutator 8 to advance. When the key corresponding to the letter Q is released, the universal bar 44 returns to its normal position, causing contact lever 17 to reestablish contact at 21 thereupon causing a substitution commutator to move forward, as described.

In Fig. 1 the control commutators were provided with rings of but six contact surfaces on each face, whereas the substitution commutators were provided with rings of 26 contact surfaces. There is, however, no reason why the substitution and the control commutators should not be identical in this regard, thus providing for their interchangeability and greatly increasing the keying possibilities of the cryptograph.

In Fig. 2 is shown how the homologous elements of Fig. 1 may be modified to accomplish this effect. End plate 304 and the commutators 6, 7, 8 now bear rings of 26 contacts instead of rings of only 6 contacts. Contact 27 remains a single contact for the entrance of the current into the control commutators, leaving 25 contacts on end plate 304 for the emergence of the current from the control commutators. These 25 contacts are ~~then~~ joined in 5 sets of 5 contacts each, to the five conductors 37, 38, 39, 40 and 41.

Other groupings in respect to the numbers and identities of contacts constituting each of the five groups may be preferable, or this may be subject to variation, according to a key.

The arrangement shown in Fig. 2 provides a sequence of keying impulses which will not begin to repeat until control commutator 6 has made a complete revolution, or after $26 \times 26 \times 26 = 17,576$ depressions of the universal bar, corresponding to the encipherment of exactly 17,576 letters of plain-text. Due to the irregular manner in which the internal connections of the control commutators are made, the substitution commutators will be caused to rotate through unequal angles, so that when the second cycle of the control commutator unit is begun, the alignment of the substitution commutators will differ from its initial alignment. As a consequence of this new alignment of the substitution commutations, the period of the sequence of selection of substitution alphabets will be greater than 17,576 by some multiple of that number, depending upon the wiring of the three control commutators and the manner in which the contacts of end plate 304 are connected to the selector magnets. This substitution period is therefore one of tremendous length.

A third form of the invention is schematically depicted in Figure 3. From a cryptographic standpoint the essential difference between this form and the first described form lies in the utilization of a single commutator unit, which serves both as a substitution commutator unit and as a control commutator unit, the two functions being performed by independent, concentric rings of contacts borne on the same commutators. In Fig. 4 there is shown a side view of one such commutator. In this figure there is on each face of the commutator an outer ring of 26 equidistant contacts, ^{for the sake of clarity,} ~~of which only six indicated by numeral 48, are shown,~~ and a concentric inner ring also of 26 equidistant contacts, ~~of which only six indicated by numeral 49, are shown.~~ The contacts 48 of the outer ring on one face are irregularly connected by insulated conductors 50 to the contacts 148 of the outer ring on the other face. Similarly the contacts 49 of the inner ring on one face are irregularly connected by insulated conductors 150 to the contacts 149 of the inner ring on the other face of the commutator. The two rings are therefore entirely independent of each other, though they

are both carried on the same commutator. Commutators of this type will hereinafter be termed double-ring commutators.

Reference is now made to Fig. 3 in which this embodiment of the invention is also shown merely in schematic form. 101, 102, 103, 104 and 105 are double-ring commutators mounted on a common shaft 20, separated by separators 305, 306, 307, and 308. Means are provided to cause the commutators to be closely pressed against one another so that positive electrical contact may be made between adjoining commutators and separators and between commutator 101 and end plate 301. A side elevation of end plate 301 is depicted at the left in Figure 3, showing the connections between the contacts thereon and the selector magnets 9, 10, 11, 12, and 13. The dotted line through the commutators 101 to 105 indicates the path of the current through the inner rings of contacts while the continuous line marks the path through the outer ring of contacts.

The sequence of events during the encipherment of a letter is as follows: When main switch 36 is closed, at the commencement of operation, a circuit is set up as follows: From battery 16 through closed main switch 36, conductor 51, contact lever 17, contact lever 17, closed contact 21, conductor 26, inner-ring contact 127 of end plate 301, into commutators 101 to 105 and out of them along broken-line path to another inner-ring contact 128 of end plate 301, thence along conductor 38, through selector magnet 10, along conductor 43, back to battery 16. When selector magnet 10 is momentarily energized it causes commutator 104 to be angularly displaced $1/26$ of a revolution, thus setting up a path through the commutators for enciphering the first letter, say letter A. When key A is depressed, universal bar 44 is caused to move downward, moving contact lever 17 away from contact 21 and allowing current to pass from battery 16 along conductor 23, through closed contact 22, contact lever 18, conductor 24, outer-ring contact 29 of end plate 301, into the commutators through which it follows the continuous line and returns via outer-ring contact 30 of end plate 301, conductor 25, contact lever 19, closed contact 47 to indicating device 14, conductor 43 and back to battery 16. After the letter Q, corresponding to indicating device 14, has been recorded, key A is released and breaks contact at 22, at the same time allowing universal bar 44 to return to its normal position. When universal bar 44 returns to its normal position contact 21 is closed reestablishing a circuit through the inner-ring contacts

of the commutators. But commutator 104 having been displaced an entirely new path through the commutators is now available for enciphering the letter A, if it is again to be enciphered.

The decipherment of the letter Q takes place in an analogous manner. The machine having been reset to the key, the closing of main switch 36 as before causes a current to flow through one of the inner-ring contacts to selector magnet 10, moving commutator 103 one step forward. Depression of key Q establishes a circuit as follows: Battery 16, closed switch 36, conductor 23, closed contact 42, contact lever 19, conductor 25, outer-ring contact 30, thence along the continuous line into, through and back through the commutators, emerging at outer-ring contact 29, conductor 24, contact lever 18, closed contact 46, indicating device 15, corresponding to the letter A, conductor 43, back to battery 16. When key Q is released, universal bar 44 returns to its normal position and again a circuit is established through the inner-ring contacts of the commutator. But since commutator 103 has been displaced, a new path is now available for deciphering the letter Q if the Q key is again depressed.

The period of the sequence of alphabet selection produced by this arrangement is variable and will depend upon four variable factors, namely (1) the wiring of the inner rings of contacts of the double-ring commutators; (2) the horizontal permutation of these commutators on the shaft; (3) the alignment of the commutators and (4) the manner in which the inner ring of contacts on end plate 301 are connected to the selector magnets.

In Fig. 5 the invention as regards double-ring commutators to perform substitution and control functions is embodied in a cryptograph of the first category as briefly described in general terms in the first part of this specification. It will be recalled that in cryptographs of this category, there are two end plates of identical construction and a reversing switch which, when set in the enciphering position, connects the switches of the keyboard to the contacts of one of the end plates, say the right-end plate, and the indicating devices are connected to the contacts of the other end plate, say the left-end plate; while when set in the deciphering position, the reversing switch reverses the order of connections between the switches of the keyboard, contacts of the end plates, and the indicating devices, so that the keyboard switches are now connected to the left-end plate and the indicating

devices are connected to the right end plate.

Accordingly in Fig. 5 there is shown a keyboard 52, a bank of indicating devices 53, a left end plate 301, a right end plate 302, and a reversing switch 54, together with other parts homologous to those shown in the preceding figures. Only ^{certain} ~~some~~ keys of the keyboard and ^{of the} ~~some~~ indicating devices of the bank of indicating devices are shown in circuit relationship, it being understood that the remaining keys and indicating devices are connected in homologous manner.

Assuming that the cryptograph is to be operated for enciphering, the switch 54 is set to enciphering position, which arranges for circuit continuity along the continuous lines 55 to 58. The main switch 36 is now closed and a circuit is established as follows: Battery 16, closed switch 36, conductor 23, universal bar switch lever 17, closed contact 21, conductor 26, inner-ring contact 127 of right end plate 302, through the commutator unit, to inner-ring contact 128 of left end plate 301, conductor 38, selector magnet 10, conductor 43 back to battery 16. Commutator 104 is angularly displaced one step. Key A is now depressed. The circuit through the inner-ring of contacts of the commutators is now broken, as universal bar 44 breaks the contact at 21. At the same time a circuit is established through the outer-ring of contacts of the commutators, as follows: Battery 16, closed switch 36, conductor 23, contact lever 18 operated by key A, closed contact 22, conductor 24, through the reversing switch 54 along conductor 55, conductor 224, outer-ring contact 29 of right end plate 302, into and through commutators 105, 104, 103, 102, 101, via their outer-ring contacts, an outer-ring contact 229 of left end plate 301, conductor 243 to the reversing switch 54 through the latter along conductor 58, thence along conductor 343, indicating device 14, corresponding to the letter Q, conductor 43 to battery 16. When key A is released, universal bar 44 returns to its normal position, reestablishing contact at 21. Again a current flows through the inner ring contacts of the commutators, entering at contact 29 but now emerging at some contact other than 128 on left end plate 301, since commutator 104 has been displaced. A selector magnet is energized, and a new path is set up for the passage of the next enciphering current if A is again depressed.

If key Q is depressed, instead of key A, the circuit is as follows:

Battery 16, closed switch 36, conductor 23, switch lever 19, closed contact 42, conductor 25, through reversing switch along path 57, conductor 325 to an outer-ring contact 30 of right end plate 302, thence through commutators to an outer-ring contact 230 of left end plate 301, conductor 425, through the reversing switch along path 59, conductor 443 to some one of the indicating devices of 53, say the one corresponding to letter Z. In other words, the relationship between A and Q is not reciprocal, when the cryptograph is set at the enciphering position, as is the case in the preceding figures. Here A in plain text gives Q in cipher, but Q in plain text gives Z in cipher.

In order to effect decipherment, the reversing switch 54 must be set for the deciphering function. This causes the paths through the reversing switch 54 to follow along the dotted lines instead of along the continuous lines. The operation immediately subsequent to closing main switch 36 is now exactly the same as before, when the encipherment of letter A was described. This is because the circuits to the selector magnets are associated with the inner-ring contacts of the commutators, and these contacts are not connected to any of the contacts in the reversing switch 54. In the first enciphering operation, the letter A was enciphered by Q. The decipherment of Q will now be followed. Depressing the Q key causes universal bar 44 to break the circuit at 21, as before, but the substitution circuit is now partly different from what it was when key A was depressed in encipherment. The circuit is now as follows: Battery 16, closed switch 36, conductor 23, contact lever 19, closed contact 42, conductor 25, through reversing switch 54 along dotted path 257, conductor 243, outer ring contact 229 of left end plate 301, through the outer-ring contacts of the commutators to an outer ring contact 29 of right end plate 302, conductor 224, through reversing switch 54 along dotted path 255, conductor 225, indicating device A, conductor 43, to battery 16. Thus Q in cipher yields A in plain language. If key A is depressed instead of Q, the control circuit is exactly the same as when Q was depressed but the substitution circuit is as follows: Battery 16, closed switch 36, conductor 23, contact

lever 18, closed contact 22, conductor 24, through reversing switch 54 along dotted path 255, conductor 525 to an outer-ring contact of left end plate 301. The current will emerge at some outer-ring contact of right end plate 302, thence go to and through the reversing switch 54, and from there it would go to some one of the indicating devices of 53, the exact one not being indicated in the figure. In any case it will be the plain-text letter which was enciphered when the cryptograph was in the homologous position in the enciphering cycle.

A fifth embodiment of the invention utilizes single-ring commutators to serve both as substitution commutators and control commutators by means of a gang switch of 26 contacts inserted in the circuits through the commutators. Figure 6 shows a schematic diagram of this form of the invention.

Having now particular reference to Figure 6, with the exception of the gang switch and relays which will be described presently, the elements shown therein are similar in construction and function with the corresponding elements shown in the preceding figures. Gang switch 85 is merely a device for breaking one complete set of 26 contacts simultaneously and at the same time making another set of 26 contacts simultaneously. It is operated by magnet 83 and associated relays. The action of this form of the invention is as follows: At the beginning of operation, switch 36 is closed, setting up circuits through relays 113 and 114, as follows: battery 16, conductors 23, 111, switch lever 17, closed contact 72, conductor 112 relays 113 and 114, conductor 124, to battery 16. Relays 113 and 114 are energized, causing armatures 80 and 108 to establish contact at 81 and 109, respectively. By means of a mechanical locking arrangement, once armature 80 has been attracted by relay 113 the contact established at 81, is locked until released by the action of relay 68; similarly when armature 108 of relay 114 has been locked into contact position at 109, it stays locked until relay 110 is energized. Consequently, although contact 72 must be closed in order to establish contact at 81 and 109, after the latter contacts have been established they will remain so even if contact 72 is broken by depressing universal bar 44. When key A is depressed universal

bar 44 causes contact lever 17 to make contact with contact 21, setting up the following circuit: from source of power 16 through conductors 23, 111 and contact lever 17, to closed contact 21 through conductor 79 and locked lever 80 of relay 113 to contact 81, thence through conductor 82 through gang-switch magnet 83 and conductors 116, 124 back to source of power 16. When gang-switch magnet 83 is energized, armature 86 is attracted, causing gang-switch 85 to disengage a lower set of twenty-six contacts and to engage an upper set of twenty-six contacts. Switch levers 88, 188, 288, 388, 488 and 588 are five of the set of 26 switch levers controlled by gang switch 85; contacts 90, 190, 290, 390, 490 and 590 are five of the set of 26 lower contacts controlled by the switch levers of the gang switch 85; contacts 91, 191, 291, 391, 491 and 591 are five of the set of 26 upper contacts controlled by the switch levers of the gang switch 85. Referring to contacts 91 and 191, which have been closed by energizing gang-switch magnet 83 as noted above, there is set up a circuit as follows: from source of power 16 through conductor 23 to closed contact 46, (the key A still being depressed) through contact lever 18 and conductor 119 to closed contact 91, through contact lever 88, and conductor 76 to a contact 29 on end plate 301, commutators and separators 1, 305, 2, 306, 3, 307, 4, 308, and 5. Commutator 5 is a reversing commutator, and therefore the current goes back through the commutators and separators 5, 308, 4, 307, 3, 306, 2, 305, 1, and returns to end plate 301, emerging at contact 30 on end plate 301; thence along conductor 84 and contact lever 188 to closed contact 191, through conductor 93, contact lever 19, closed contact 42 along conductor 121, to indicating device 14, thence along conductor 43 to relay magnet 68 and back along conductor 77 to battery 16.

When indicating device 14 is energized, a type bar is caused, by means not shown, to print the letter Q, ~~as shown in the diagram~~ which ^{is} ~~indicates~~ the cipher equivalent of the plain-text letter A. When relay magnet 68 is energized, contact lever 80 disengages contact 81 and engages contact 100, deenergizing switch control magnet 83 and allowing gang switch 85 to disengage the upper set of 26 contacts, among which are contacts 91 and 191, and engage the lower set of 26 contacts, among which are 90 and 190. This sets up a circuit as

follows: battery 16, conductors 23 and 111, universal-bar contact lever 17, closed contact 21, conductor 79, contact lever 80, contact 100, conductor 122, selector magnet 13, conductor 106, closed contact 190, contact lever 188, conductor 84, contact 30 on end plate 301, to, through and back through commutators 1 to 5, contact 29, conductor 76, contact lever 88, closed contact 90, conductor 107, contact lever 108, closed contact 109, relay magnet 110, conductors 123 and 124, back to battery 16.

When selector magnet 13 is energized, commutator 1 is angularly displaced through $1/26$ th of a revolution, and a new set of circuits is formed in the commutator unit. Relay magnet 110 having been energized, contact lever 108 is caused to disengage contact 109. This breaks the circuit through the selector magnets and prevents energizing selector magnet 13 a second time. No further action of any part can take place until the two relays 113 and 114 are again actuated. This happens when key A is released, which establishes a circuit as follows: battery 16, conductors 23 and 111, contact lever 17, closed contact 72, conductor 112, magnets 113 and 114, back to battery 16. As explained above, armatures 80 and 108 are locked in contact-making positions at 81 and 109 until another key of the keyboard is depressed, causing the device to operate in the same manner as hereinbefore described.

M-161

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER

MEMORANDUM for

Office File

Drawings + specs on SIS DE 11

The [attached] was disclosed to Cndr.
MacFarlan + Lieut. Wenger, Code + Signal
Section, Navy Dept on Oct 21, 1935.

Oct. 21, 1935.

W. F. Friedman ✓

Again described + disclosed to Lts Wenger,
Harper + Cndr Mc Claran on Oct 31, 1935 at Navy Dept.

Again described to Lts. Wood + Dugan at this
office on Nov 1, 1935.

W. F. F.

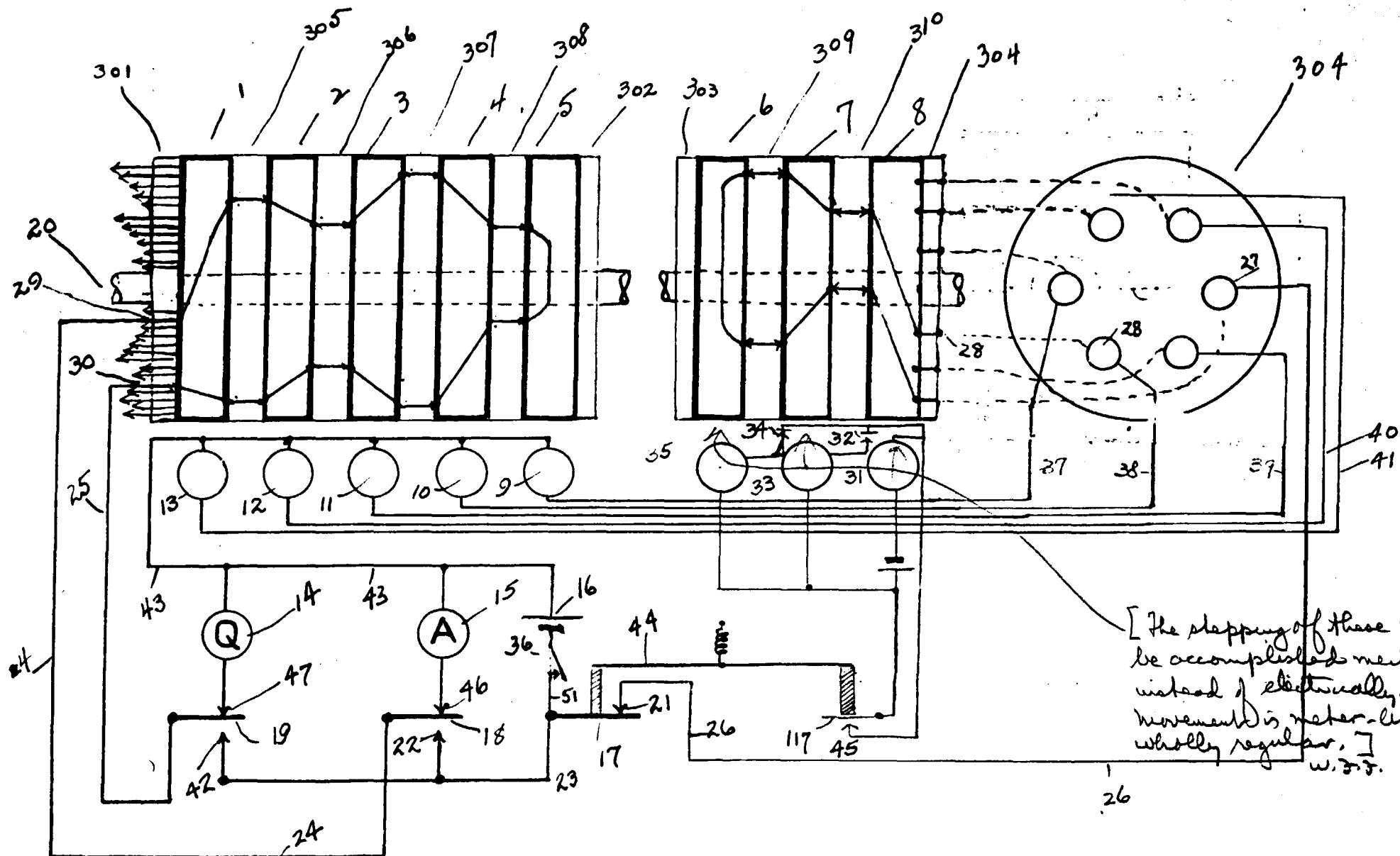
Figs. 1
to

Fig. 7 (incl)

1-6, inc

See memo of
Nov 27, 1935 to
(Rowe)

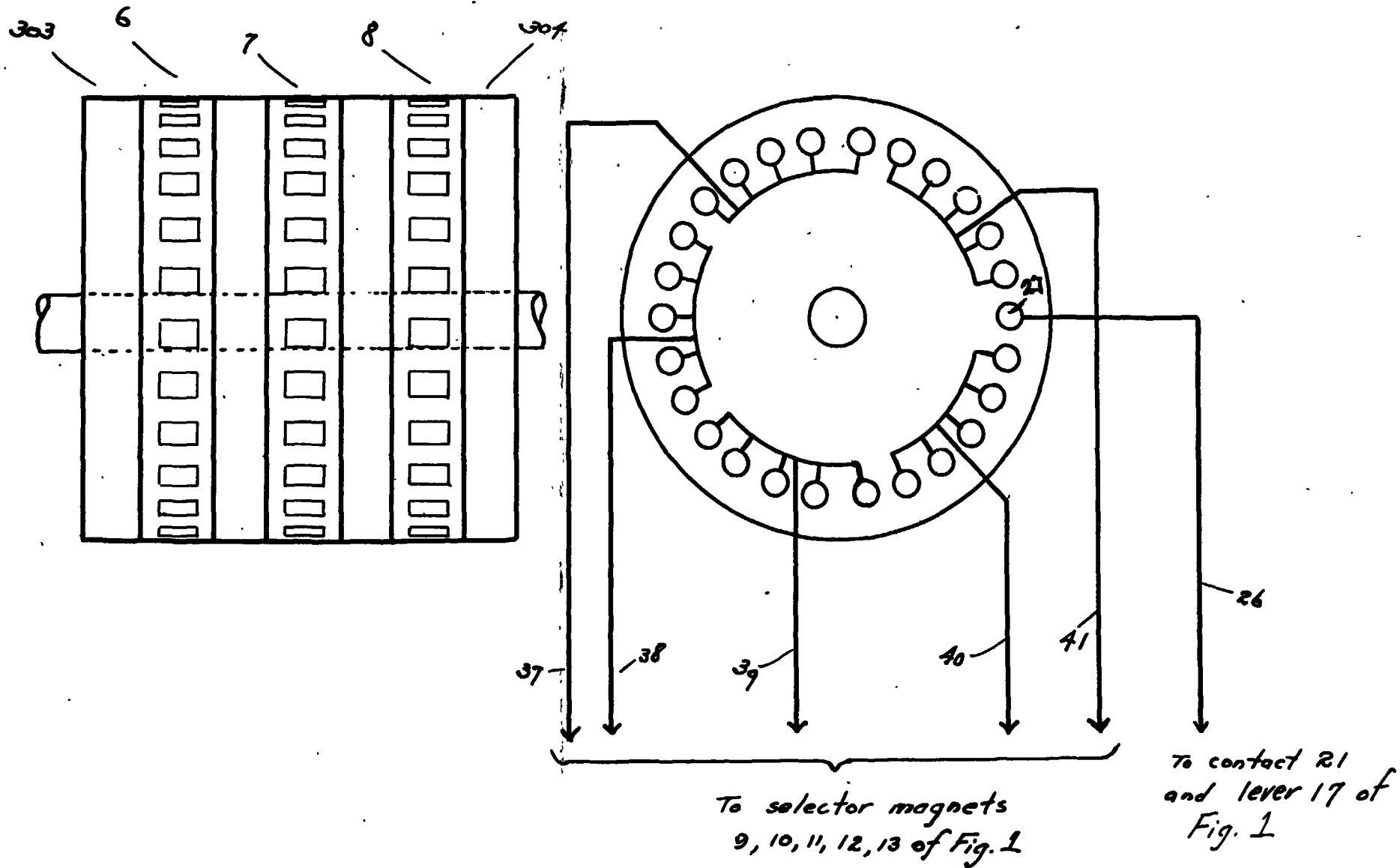
The originals
of these drawings
are in a separate
large envelope - too
large to go in this file.
The envelope is contained
in same cabinet as this
file. J.



[The stepping of these wheels can be accomplished mechanically instead of electrically. Their movement is meter-like and wholly regular.]
W.F.F.

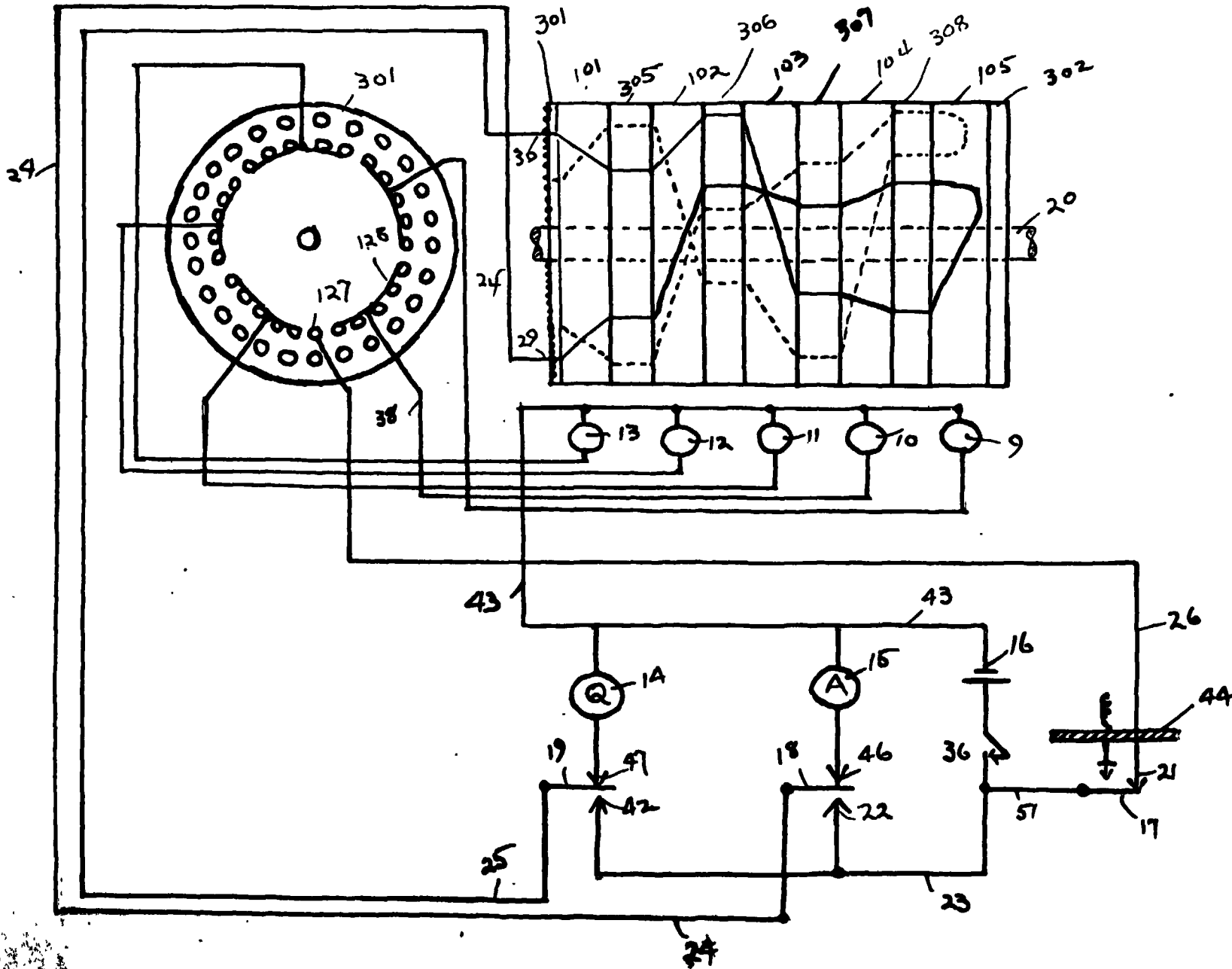
Fig. 1.

Inventors:
Washington, D.C. Aug. 31, 1935
William F. Friedman
Frank B. Rowlett



Inventors:
 Washington, D.C.
 Aug 30, 1935
 William F. Friedman
 Frank B. Rowlett

Fig. 2



Inventors:
 Washington, D.C.,
 Aug. 31, 1935
 William F. Friedman
 Frank B. Rowlett
 by J.

Fig. 3

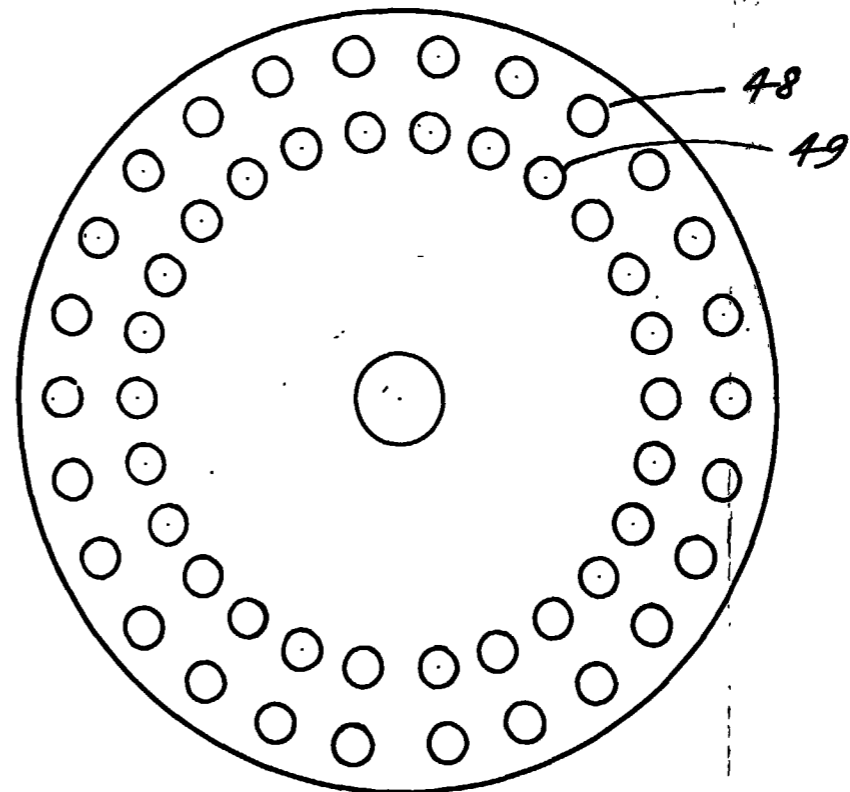
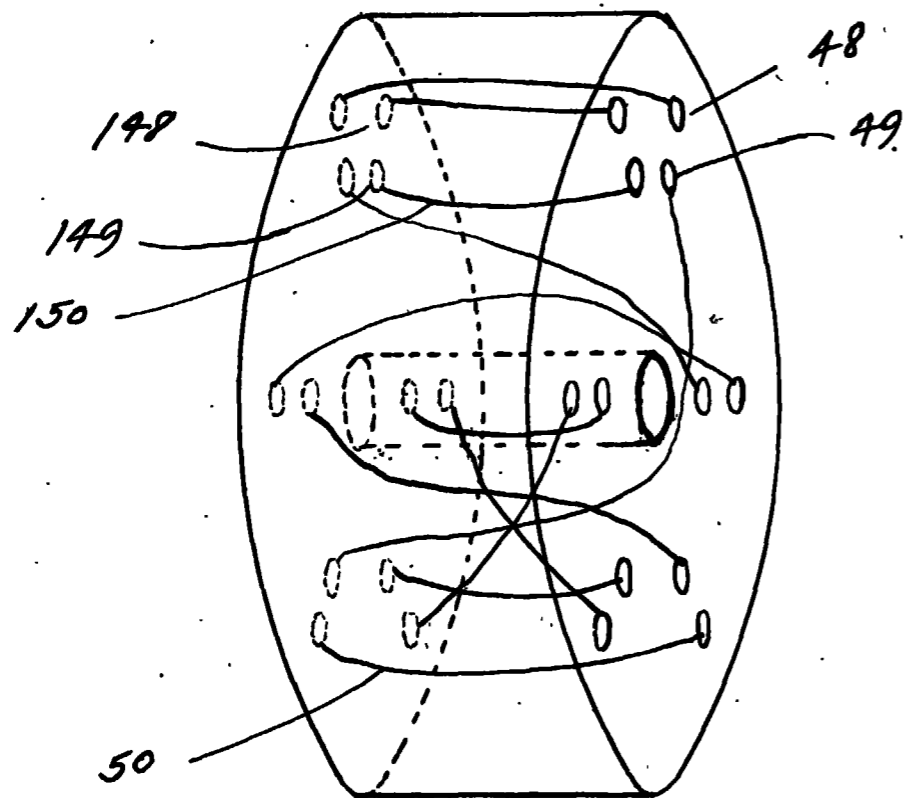


Fig. 4

Inventors:
Washington, D.C. Aug 31, 1935
William F. Friedman
Frank B. Rowlett

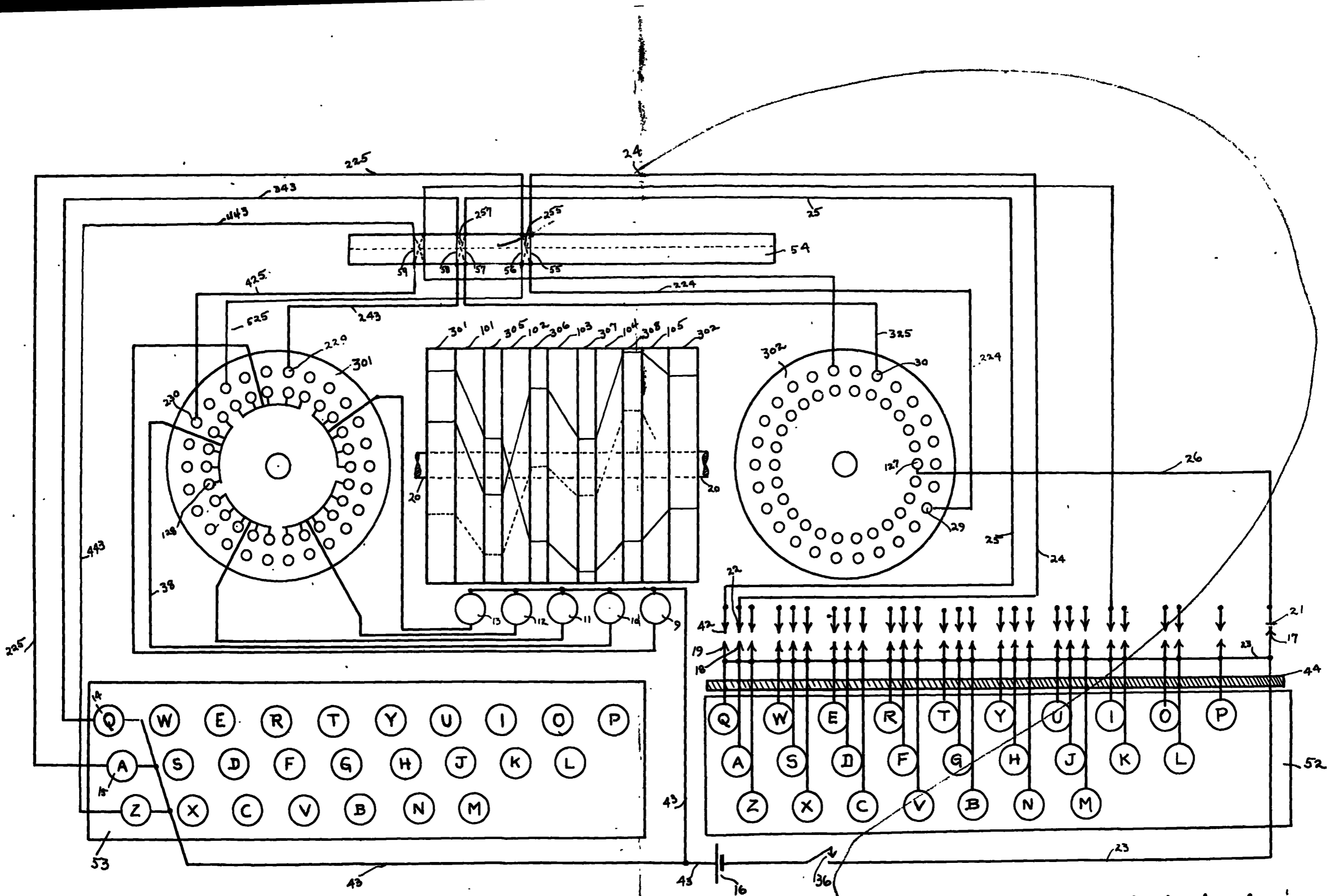


Fig. 5

[In this drawing the enciphering-deciphering relationship is not reciprocal, but is like that in M-134 T2. Hence an enciphering-deciphering switch is necessary, as in M-134 T2.]
W.F.F.

Inventors:
Washington, D.C., Aug. 31, 1935
William F. Friedman
Frank B. Rowlett

To rest of upper contacts of key switches, homologous to key switches 74 and 174

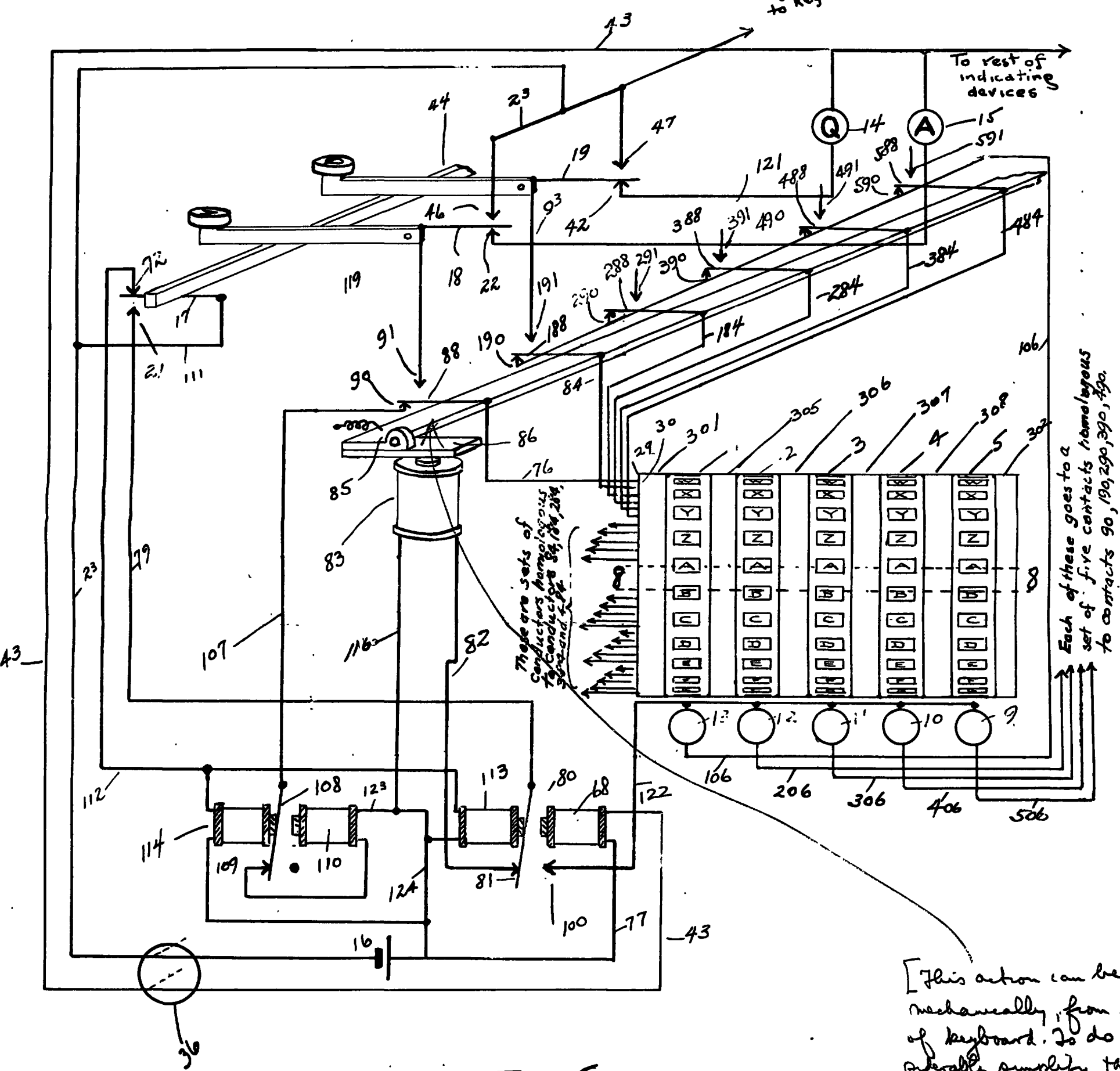
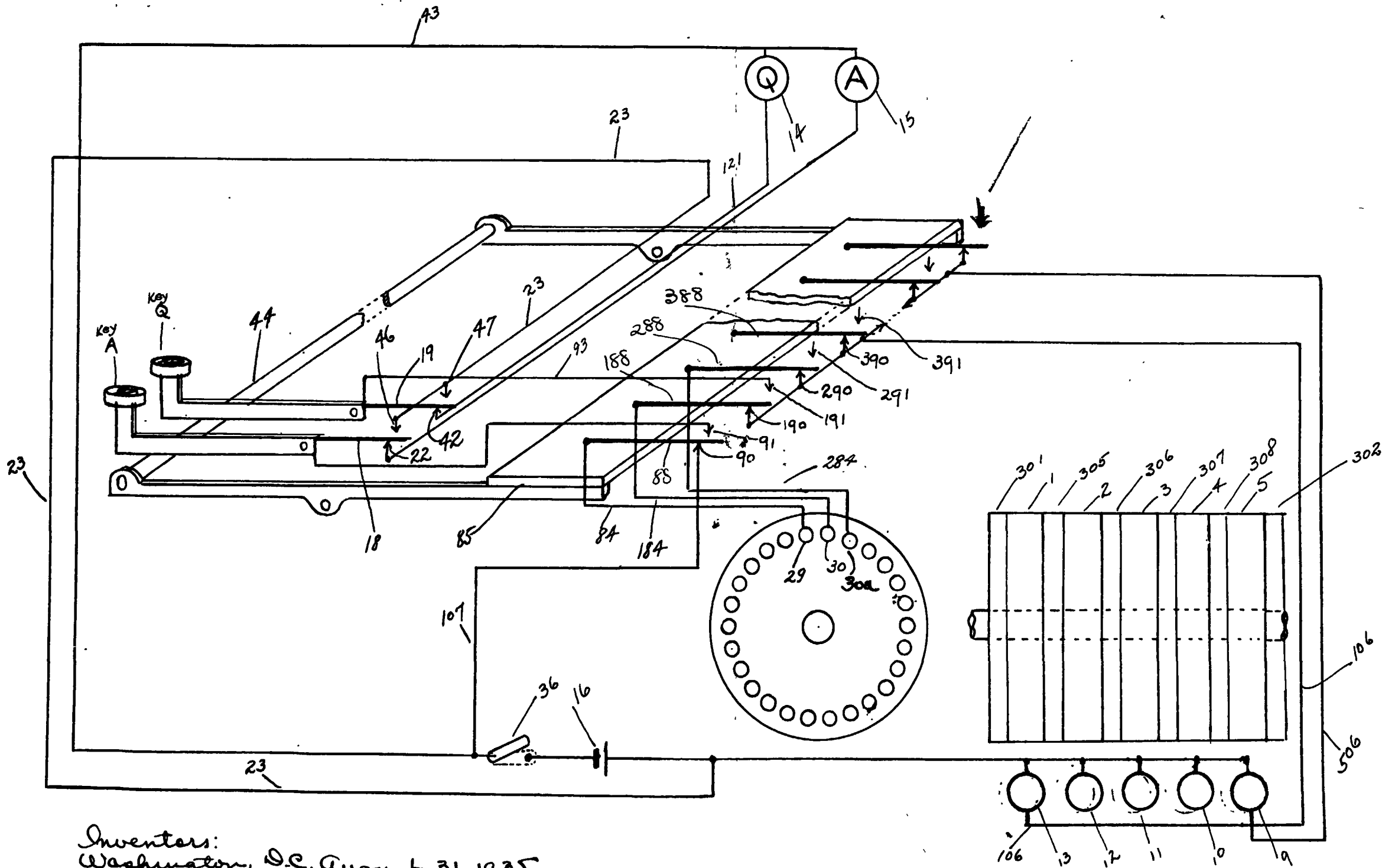


Fig. 6

[This action can be accomplished mechanically, from universal bar of keyboard. To do so would considerably simplify the circuit.]
W.S.F.

Approved:
Washington, D.C., Aug. 21, 1931
William F. Friedman
Frank B. Rowlett

Changes 1 (add)



Inventors:
 Washington, D.C. August 31, 1935
 William F. Friedman
 Frank B. Rowlett

Fig. 7